How Wi-Fi Works

Securing the Air Waves

Sean Campbell

Adam Ebbeka

April 23rd, 2007

1. Introduction

Wi-Fi networks are not much different from their wired cousins when it comes down to the OSI model. The only difference is that the physical layer consists of radio signals rather than copper wiring or optic fiber cables. The wireless network adapters operating on the data link layer turn the digital information into radio waves and back. Beyond this, it's the same Ethernet that we all know.

Wireless technologies present many advantages and disadvantages. The advantages are clear, no wires. The disadvantages aren't so obvious. In a wired network, especially a switched wired network, you know where your data is going. It's going straight to its destination. Although your information can be intercepted, it's not as easy as with wireless. Everything you send and receive over Wi-Fi is easily receivable anywhere within the range of the signal. Luckily there are security measures and encryptions available, but unfortunately most public Wi-Fi networks are not secure and the users probably don't think twice about the information they're broadcasting to the world.

2. How Wi-Fi Works

In 1997, the IEEE (Institute of Electrical and Electronics Engineers) created the 802.11 standard for networks using either radio waves or infrared light. Over the years, many different variances of the protocol have been defined, such as 802.11a, b and g. The differences between the standards are mainly speeds and radio frequencies. Most use a frequency of 2.4 GHz. Ranges are 25 to 100 meters, depending on the protocol, equipment, and environment.

2.1 Physical Layer

Wi-Fi uses a method called spread spectrum to transmit over a wide band of frequencies. The other option, transmitting over a narrow band, is much less efficient. Not only does spread spectrum require less power, but it is less prone to interference. Two types of spread spectrum are used by Wi-Fi: FHSS (frequency-hopping spread spectrum) and DSSS (direct-sequence spread spectrum). FHSS was used on older systems, most use DSSS now.

DSSS spreads the signal across a 22 MHz channel. Each bit of data is put into redundant patterns called chips before being transmitted. Any interference that may disrupt a relatively small portion of the channel can be rebuilt upon decoding thanks to the pattern redundancy. Handshaking is used to ensure packets are transmitted completely successfully.

Different regions of the world have different laws regulating Wi-Fi. In North America, Wi-Fi operates between 2.4000 and 2.4835 GHz, on 11 different channels. You'll notice that in order for DSSS to cover a 22 MHz spread, there is some overlap between channels. Interference between multiple Wi-Fi networks will cause a decrease in performance, so it's best to operate the networks about six channels apart from each other. For instance, three networks on channels 1, 6, and 11 would not have any interference.

Channel	Freq. (MHz)	Channel	Freq. (MHz)
1	2412	7	2442
2	2417	8	2447
3	2422	9	2452
4	2427	10	2457
5	2432	11	2462
6	2437		

2.2 Data-Link (Media Access Control) Layer

Every transmitted packet contains a preamble. 802.11 preambles are 144 bits long, consisting of 128 bits used for synchronization and a 16 bit start-of-frame field. Next a 48 bit header is transmitted containing typical network packet information such as speed, packet length and a checksum. A shorter 72 bit preamble is also an option. Both work equally as well, but are not compatible with one another.

For collision avoidance, 802.11b uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Before transmitting, nodes listen to see if any other nodes are transmitting. If nothing is heard, it waits a short random amount of time, listens again, then transmits. If it

doesn't hear back from the receiver, it assumes there was a collision and retransmits the packet. In the case of a collision, the CSMA/CA tells all but one of the transmitting nodes to stop.

2.3 Operation Modes

There are three main modes that Wi-Fi can operate in. The most common is infrastructure mode. In this mode, an Access Point is wired into a network and several remote users can connect to it. This is the most secure mode, because you are likely to know what you're connecting to, plus the single Access Point can have complete control over who is allowed to connect.

Another common mode is Ad-hoc. In Ad-hoc mode, there is no base Access Point. Wi-Fi devices communicate directly to one another. This is common with small Wi-Fi enabled devices such as cell phones, PDAs, and even newer mp3 players that have no need for an access point to transfer small amounts of data from one device to another. Beyond this, Ad-hoc doesn't have much of a use in a full scale networking operation.

Lastly, used typically only for monitoring traffic, is monitor mode. While operating in monitor mode, a Wi-Fi device receives every packet it can find passing through the air waves. This is similar to operating in promiscuous mode on a wired LAN. The Wi-Fi device doesn't ever connect, or even notify anything of its presence. It simply listens. With monitor mode, it is very easy capture packets on an unsecured network, making it all that more important to think twice before sending vital information to potentially every Wi-Fi device within 100 meters.

3. Security

As easy as it is to intercept packets out of the air, security is extremely important with Wi-Fi. Unlike switched wired networks, there's no way with wireless to send your packets to just one destination. Anyone with a Wi-Fi device capable of operating in monitor mode can intercept every packet you transmit and receive.

3.1 Authentication

The 802.11 standard has two ways of authenticating users, Open System authentication and Shared Key authentication. In Open System Authentication, no true form of identification is

used. It is a wide open network that anyone can join. The only requirement is that the client provides its MAC address. This form of authentication is the only form required by the 802.11 standard.

Shared Key authentication accepts clients with knowledge of a secret key. A "nonce" is generated by the Access Point and sent to the client. The client must encrypt the nonce using the secret cryptographic key, and then return the encrypted nonce to the Access Point. The client is given access if the decryption is the same as the original nonce transmitted. This method is not completely fool proof, because it is only a one way authentication. The client has no way of knowing that the Access Point is really who it says it is.

3.2 Privacy

Currently the most common form of Wi-Fi security is WEP (wired equivalent privacy), originally intended to give wireless the same security as a wired network, which in reality isn't really the case. WEP uses a symmetric-key to generate a data sequence, which is then exclusive or-ed with the data to be transmitted. Key size by definition is 40 bits, though many manufactures have increased it for greater security. 128 bit WEP is very common. Although data is encrypted with WEP, it can still be intercepted and decrypted by brute force or other methods.

WPA (Wi-Fi Protected Access) and WPA2 were created as a more secure method of protection to fix the flaws of WEP. The biggest improvement is the Temporal Key Integrity Protocol (TKIP), which automatically changes the key. This dynamically changing key is optional, as there is also a less secure pre-shared key mode which works similar to WEP. Another feature making WPA superior to WEP is the MIC (Message Identity Code), which is basically a frame counter. This prevents replay attacks in which an attacker can capture an encrypted packet containing information such as a password, then attempt to gain access by posing as someone else and retransmitting that same packet when asked for a password.

4. 802.11n - The Next Generation of Wi-Fi

As with all forms of technology, Wi-Fi is evolving and there has become a need for faster speeds and longer ranges among networks. The next big thing in wireless computing is called 802.11n. This new IEEE WLAN standard is currently under development and claims to deliver a whopping four-fold increase in network throughput. Not only that, but the standard is rumored to significantly increase the range at which any 802.11n-based Access Point can operate as well. Lastly, the new standard claims to be 100% backwardly compatible with existing WLAN standards (802.11a/b/g). Needless to say, the future looks very bright for the already popular home/business Wireless LAN.

The major boost in performance is a result of a new technology called multiple-input multiple-output (MIMO). This technology uses multiple antennas on both the sender and receiver sides to achieve Spatial Division Multiplexing (SDM). Essentially, SDM divides separate data streams among antennas which can simultaneously send/receive data through a common spectral channel of bandwidth. For this to work, each antenna must have a separate radio frequency and analog-to-digital converter. In short, more antennas means more bandwidth. The idea, while new to the networking realm, is actually an old one when we think about the similarities between multiple antennas and multi-core processors. The idea of parallel computing power has been extended to encompass Wi-Fi data transmission.

Another way that 802.11n improves in performance from its predecessors is in the proposed extension of range in bandwidth channels. The new standard supports both 40 MHz and 20 MHz channels, as opposed to the 22 MHz channels of 802.11b and g. It has been shown that one 40MHz channel can provide over twice the usable bandwidth than two 20MHz channels. Aside from the performance increase, the use of 40MHz channels keeps hardware costs down by reducing the number of antennas and thus reducing complexity. The only downside to these wider channels is the increased interference between overlapping networks.

The improvements in performance discussed thus far have come from modifications to the Physical (PHY) layer. 802.11n will also take advantage of tweaks to the Medium Access Control (MAC) layer. Some of the tweaks are direct results of the new hardware additions:

managing antenna configurations, channel bandwidths, channel selection, etc. Others are slight variations of preexisting procedures. For example, PHY headers have always been used, but will now have to be extended in length in order to account for all of the new configurations associated with the new hardware. This length increase leads to greater total overhead. One way 802.11n combats this is by implementing aggregate exchange sequences. This involves combining multiple MAC PDUs (Protocol Data Units) into a single PHY PDU. The advantage is that the system doesn't have to send a separate transfer for each MPDU, thus augmenting performance. In order to maximize the potential of this aggregation, the PPDU length, currently 4095 bytes, will need to be increased.

Between the bandwidth channel size and PPDU length increases, we can see that 802.11n is going to require some fundamental changes to preexisting standards. It has already been observed that early prototypes of the new standard are having some difficulty integrating with legacy systems. In his essay *802.11n Is a Gamble*, Andrew Garcia from eWEEK Labs evaluates the current state of 802.11n draft products. After many test over different hardware and driver setups, he concludes that 802.11n still has a lot of work to do in terms of stability. One reason for this inconsistent behavior is the use of 40MHz channels. Using 40MHz transmitters on the 2.4GHz band leads to collisions with legacy b and g networks causing availability issues. IEEE is aware of this problem and proposes that intelligent tweaks to the MAC layer be made in order to recognize these collisions and switch back to 20MHz channels, but currently this is still under development.

In addition to their stability issues, 802.11n devices contain security flaws. With some vendors claiming over a four-fold range increase, the network becomes available to attackers who might have been limited by spatial means in the past (for example, fenced off military bases). Another interesting security risk is the undetectability of 802.11n transmitters in Green Field mode. Legacy networks are unable to detect 802.11n devices operating in Green Field mode thus allowing an attacker to bypass monitoring systems. As mentioned earlier, an 802.11n access point with a 40MHz channel would interfere with other legacy networks in the area causing network connectivity issues. This would allow an attacker to bring the functionality of a network to its knees. This issue should be resolved once n-based devices are smart enough to detect

channel collisions. The Green Field mode rogue threat can also be fixed with future driver updates. Unfortunately there isn't much one can do as far as the increasing range of wireless networks goes. Hopefully, as the range increase in Wi-Fi technology becomes better known, more people will shy away from range-based security. With the ease of use of WEP pass-phrase encryption today, there is really no reason not to utilize it.

5. Wi-Fi Security In and Around Downtown Lincoln

We set out with a laptop loaded with the packet sniffing program called *Wireshark*, and a Wi-Fi card in Monitor Mode, to find out how secure wireless networks are in the area. At one point we found 17 networks all in one area. Imagine the interference users must have been getting... The shocking thing was that only seven of them were secured, and several were extremely unsecured Ad-Hoc networks. We easily monitored these networks and captured packets from them. While monitoring UNL's campus wide Wi-Fi network, we successfully received Instant Messenger conversations. Clearly, if we could capture IM packets, we easily could have captured packets containing passwords and credit card numbers that criminals would be looking for, had they been passing through the air waves at the time.

6. Conclusion

Wi-Fi has much greater security challenges than wired networks. The only control over packet destination is the range of the signal. Luckily Wi-Fi technology is evolving and better methods of authentication and encryption are being invented and implemented.

Unfortunately, security is not always convenient. Imagine a public Wi-Fi network such as one found in a coffee shop. How convenient would it be to have to tell every customer a 128 bit key? The key would have to be changed daily, but still this wouldn't do any good. The key would be public information. Any attacker could get the key and decrypt packets.

For this reason alone, packet encryption just doesn't seem to work in a public situation. It works great in a private network where only trusted people are given the key. So, when a secure network isn't an option, the security is left up to the user. Data encryption at higher levels helps,

such as SSL encrypting information sent over the web, or using SSH as opposed to telnet. Of course, the most secure option is to simply not send vital information out over public airwaves.

References

Ellison, Craig. "Getting a Leg Up on 802.11n." ExtremeTech. 7 Oct. 2004. 21 Apr. 2007. <http://www.extremetech.com/article2/0,1697,1675706,00.asp>.

Garcia, Andrew. "802.11n Is a Gamble." eWEEK Labs. 23 Jul. 2006. 21 Apr. 2007 <http://www.eweek.com/article2/0,1895,1992140,00.asp>.

Karygiannis, Tom, and Les Owns. Wireless Network Security. NIST, 2002.

Ross, John. The Book of Wi-Fi. Oreilly & Associates Inc, 2003.

Wilson, James M. "Quadrupling Wi-Fi speeds with 802.11n." DeviceForge.com. 9 Aug. 2004. 21 Apr. 2007. <http://www.deviceforge.com/articles/AT5096801417.html>.

Wright, Joshua. "Security issues with pre-802.11n wireless gear." Network World. 13 Nov. 2006. 21 Apr. 2007 <http://www.networkworld.com/columnists/2006/111306-wireless-security.html>.